Amendments to the Claims:

A listing of the entire set of pending claims (including amendments to the claims, if any) is submitted herewith per 37 CFR 1.121. This listing of claims will replace all prior versions, and listings, of claims in the application.

Listing of Claims:

1. (Currently amended) A method for cryptographically converting an input data block into an output data block; the method including:

selecting a select permutation from a predetermined set of at least two permutations, and

performing a non-linear substitution operation on the input data block ~~using an S-box~~ based on ~~a~~ the select permutation~~, wherein the method includes each time before using the S-box (pseudo-)randomly selecting the permutation from a predetermined set of at least two permutations associated with the S-box~~.

2. (Original) A method as claimed in claim 1, wherein the set of permutations is formed such that a cryptographic weakness in one of the permutations of the set is at least partially compensated by a corresponding cryptographic strength in at least one of the other permutations of the set.

3. (Currently amended) A method as claimed in claim 1, wherein

the data block consists of n data bits and

each ~~element~~ permutation of the set of permutations is ~~a permutation on~~ a set of 2^n elements, ~~represented by Z_2^n,~~ where each non-trivial differential characteristic of each permutation in this set has a probability that is less than or equal to a maximum probability ~~of at most p_{diff}~~,

the set of permutations being formed by permutations which have been selected such that for each non-trivial differential characteristic having the maximum probability ~~with probability of p_{diff}~~ in any of the permutations, this differential characteristic has a lower probability ~~lower than p_{diff}~~ in at least one of the other permutations of the set.

4. (Original) A method as claimed in claim 3, wherein the differential characteristic has a probability equal to zero in at least one of the permutations.

5. (Currently amended) A method as claimed in claim 4, wherein $n = 4$, and ~~p_{diff} =~~ the maximum probability equals ¼.

6. (Currently amended) A method as claimed in claim 1, wherein

the data block consists of n data bits and

each ~~element~~ permutation of the set of permutations is ~~a permutation on~~ a set of 2^n elements, ~~represented by Z_2^n,~~ where each non-trivial linear characteristic of each permutation in this set has a probability of at least ~~$\frac{1}{2} - p_{lin}$~~ a minimum probability and at most ~~$\frac{1}{2} + p_{lin}$~~ a maximum probability,

the set of permutations being formed by permutations which have been selected such that for each non-trivial linear characteristic with probability ~~of $\frac{1}{2} - p_{lin}$ or $\frac{1}{2} + p_{lin}$~~ that equals the minimum or maximum probability in any of the permutations, this linear characteristic has a probability closer to ½ in at least one of the other permutations of the set.

7. (Currently amended) A method as claimed in claim ~~5~~ 6, wherein the linear characteristic has a probability equal to ½ in at least one of the permutations.

8. (Currently amended) A method as claimed in claim 6, wherein $n = 4$ ~~and $p_{lin} = 1/4$~~, the minimum probability is ¼, and the maximum probability is ¾.

9. (Original) A method as claimed in claim 1, wherein the set of permutations consists of two permutations.

10. (Currently amended) A method as claimed in claim 1, wherein ~~including performing the selection of~~

selecting the select permutation ~~under control of~~ is based on an encryption key.

11. (Currently amended) A method as claimed in claim 9, wherein ~~the selection of the~~

selecting the permutation is performed under control of ~~one~~ a bit of ~~the~~ an encryption key.

12. (Original) A computer program product where the program product is operative to cause a processor to perform the method of claim 1.

13. (Currently amended) A system for cryptographically converting an input data block into an output data block; ~~the method~~ system including:

- an input for receiving the input data block;

- a storage for storing a predetermined set of at least two permutations associated with an S-box;

- a cryptographic processor for performing a non-linear operation on the input data block using an S-box based on a permutation; the processor being operative to, each time before using the S-box, (pseudo-)randomly selecting the permutation from the stored set of permutations associated with the S-box; and

- an output for outputting the processed input data block.

14. (New) A cryptographic encoder comprising:

one or more encryption stages,

each stage of the one or more encryption stages including

a non-linear substitution module that is configured to receive a control signal and a set of data bits,

wherein

the non-linear substitution module includes a plurality of substitution boxes; and

each of the substitution boxes is configured to receive at least a subset of the control signal and a subset of the set of data bits, and:

substitutes a first output value for the subset of the set of data bits if the subset of the control signal is a first value, and

substitutes a second output value for the subset of the set of data bits if the subset of the control signal is a second value.

15. (New) The cryptographic encoder of claim 14, wherein

each stage of the one or more encryption stages further includes

an addition module that is configured to combine at least a subset of a key with a data input to provide the set of data bits to the non-linear substitution module.

16. (New) The cryptographic encoder of claim 15, wherein

the control signal includes another subset of the key.

17. (New) The cryptographic encoder of claim 15, wherein

each stage of the one or more encryption stages further includes

a transformation module that is configured to transform the output values from the substitution boxes to provide therefrom an encrypted data output.

18. (New) The cryptographic encoder of claim 14, wherein

the second output value is formed such that a cryptographic weakness in the first value is at least partially compensated by a corresponding cryptographic strength in the second output value.

19. (New) The cryptographic encoder of claim 14, wherein

the subset of the set of data bits consists of n data bits and

each of the first and second data output values is a mapping of the subset of the set of data bits to an element of a set of 2^n elements, where each non-trivial differential characteristic of each of the set of 2^n elements of the first and second output values has a probability that is less than or equal to a maximum probability;

the set of 2^n elements that provide second data output value being selected such that for each non-trivial differential characteristic having the maximum probability in the set of 2^n elements that provide the first output value, this differential characteristic has a lower probability in the set of 2^n elements that provide second data output value.

20. (New) The cryptographic encoder of claim 14, wherein

the subset of the set of data bits consists of n data bits and

each of the first and second data output values is a mapping of the subset of the set of data bits to an element of a set of 2^n elements, where each non-trivial differential characteristic of each of the set of 2^n elements of the first and second output values has a probability that is at least a minimum probability and at most a maximum probability;

the set of 2^n elements that provide second data output value being selected such that for each non-trivial linear characteristic that equals the minimum or maximum probability in the set of 2^n elements that provide the first output value, this linear characteristic has a probability closer to ½ in the set of 2^n elements that provide second data output value.